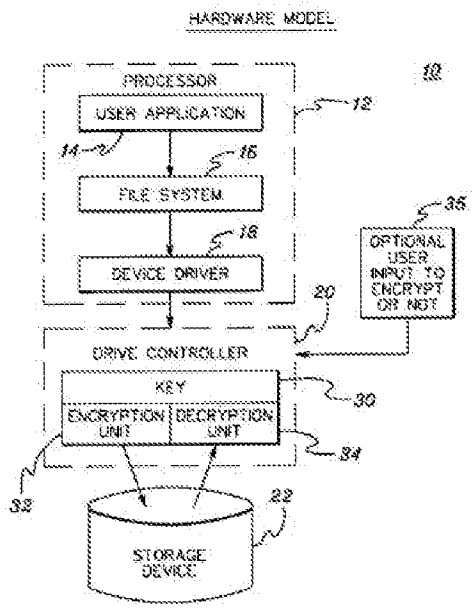
Encrypted/deencrypted stored data by utilizing disaccessible only secret key

Publication number: CN1294457
Publication date: 2001-05-09
Inventor: DETERIK M S (US); FETCOVECHY J E (US); WELHEIM G W JR (US)
Applicant: IBM (US)
Classification:
- international: ***G06F21/00; H04L9/00; H04L9/08;*** **G06F21/00; H04L9/00; H04L9/08;** (IPC1-7): H04L9/00
- European: H04L9/08; G06F21/00N9F
Application number: CN20001031477 20001020
Priority number(s): US19990427250 19991026

Also published as:
US7278016 (B1)
US2007098152 (A1)
CN1312876C (C)

Abstract not available for CN1294457
Abstract of corresponding document: **US2007098152**

Encryption and decryption of data stored from a computing system to a storage medium is disclosed wherein the processing employs a non-accessible encryption key that is unique to the computing system. The unique encryption key can be embedded in non-removable hardware of the computing system or generated, e.g., from identification numbers ascertained from non-removable hardware of the computing system. Processing includes establishing the unique encryption key, encrypting data using the unique encryption key and storing the encrypted data to the storage medium without storing the unique encryption key on the storage medium. The storage medium can comprise any non-removable or removable storage medium, including for example a computer hard drive, floppy diskette, or recordable compact disk.



[19]中华人民共和国国家知识产权局

[51]Int. Cl[7]
H04L 9/00

[12]发明专利申请公开说明书

[21]申请号 00131477.7

[43]公开日 2001年5月9日

[11]公开号 CN 1294457A

[22]申请日 2000.10.20 [21]申请号 00131477.7
[30]优先权
[32]1999.10.26 [33]US [31]09/427,250
[71]申请人 国际商业机器公司
地址 美国纽约州
[72]发明人 M·S·德特里克 J·E·费特科维奇
小G·W·威尔黑尔姆

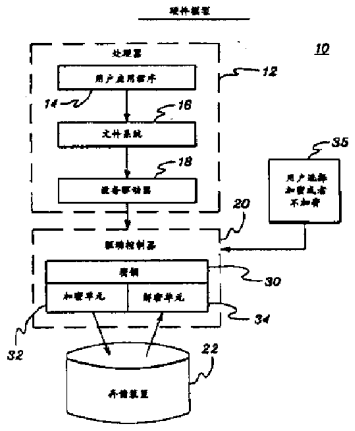
[74]专利代理机构 中国专利代理(香港)有限公司
代理人 邹光新 王忠忠

权利要求书5页 说明书7页 附图页数5页

[54]发明名称 用不可访问的唯一密钥对储存的数据进行加密/解密

[57]摘要

公开了加密和解密从计算机系统存入存储媒介的数据的一种方法,其中的处理 采用了对于该计算机系统而言是唯一的一个不可访问密钥。这个唯一密钥可以 嵌入这一计算机系统的不可拆卸硬件中,或者可以从例如该计算机系统不可拆 卸硬件的标识号产生。所述处理包括构造这一唯一密钥,用这个密钥加密数据,并将加密数据存入存储媒介,而不需要将唯一密钥存入存储媒介。这一存储媒 介可以包括任何不可拆卸或者可拆卸存储媒介,包括例如一个计算机硬盘、软 盘或者可记录光盘。



ISSN1008-4274

权　利　要　求　书

1. 一种方法，用于保护从计算机存入存储媒介的数据，该方法包括:

在所述计算机系统内构造一个唯一的密钥;

用这个唯一的密钥加密数据，产生加密数据；和

将这些加密数据存入所述存储媒介，不将唯一的密钥存入所述存储媒介.

2. 权利要求 1 的方法，其中的构造步骤包括在所述计算机系统的硬件内嵌入所述唯一密钥.

3. 权利要求 2 的方法，其中的嵌入步骤包括将所述唯一密钥嵌入所述计算机系统的驱动控制器中.

4. 权利要求 3 的方法，其中的加密步骤包括用嵌入所述驱动控制器的唯一密钥在硬件内加密.

5. 权利要求 4 的方法，其中唯一的密钥被冗余地嵌入所述计算机系统的所述驱动控制器中.

6. 权利要求 2 的方法，还包括让用户能够选择对所述数据进行加密.

7. 权利要求 6 的方法，还包括在存入所述存储媒介的每一个文件中做标记，说明所述数据文件是否需要所述计算机系统进行解密.

8. 权利要求 1 的方法，其中的加密对于在所述计算机系统上运行的用户应用程序来说是透明的，所述用户应用程序提供所述数据从计算机系统存入存储装置.

9. 权利要求 1 的方法，其中的构造步骤包括在软件中为所述计算机系统产生所述唯一密钥，所述产生步骤包括确定所述计算机系统至少一个硬件部件的至少一个标识号，并利用这至少一个标识号为所述计算机系统产生所述唯一的密钥.

10. 权利要求 9 的方法，其中的产生步骤包括在所述计算机系统一个设备驱动器初始化的时候产生所述唯一的密钥，并将所述唯一密钥储存在所述计算机系统中的易失性存储器里.

11. 权利要求 1 的方法，其中的计算机系统和存储媒介都包括计算机的一部分，其中的存储媒介包括不可拆卸计算机存储媒介或者可拆卸计算机存储媒介中的一样.

12. 权利要求 11 的方法，其中的计算机包括膝上型计算机，所述存储媒介包括所述膝上型计算机的计算机硬盘。

13. 权利要求 1 的方法，还包括从所述存储媒介取出所述加密数据，并用所述唯一密钥对加密数据解密，对在所述计算机系统上运行的用户应用程序来说所述解密是透明的。

14. 权利要求 13 的方法，其中的加密包括在硬件内用所述唯一密钥进行加密，所述硬件驻留在所述计算机系统的驱动控制器内，其中的解密包括在驻留在计算机系统的驱动控制器内的硬件内进行解密。

15. 权利要求 13 的方法，其中的加密包括在软件内用所述唯一密钥加密所述数据，这一加密是在该计算机系统一个设备驱动器中的软件内完成的，其中的解密包括在软件中用所述唯一密钥解密加密数据，这一解密还在所述设备驱动器中的软件内进行，其中的加密和解密对于所述计算机系统上运行的用户应用程序而言是透明的。

16. 一种系统，用于保护从计算机存入存储媒介的数据，该系统包括：

在所述计算机系统内构造一个唯一密钥的装置；

用这个唯一的密钥加密数据，产生加密数据的装置；和

将这些加密数据存入所述存储媒介，不将唯一的密钥存入所述存储媒介的装置。

17. 权利要求 16 的系统，其中的构造装置包括在所述计算机系统的硬件内嵌入所述唯一密钥的装置。

18. 权利要求 17 的系统，其中的嵌入装置包括将所述唯一密钥嵌入所述计算机系统的驱动控制器中的装置。

19. 权利要求 18 的系统，其中的加密装置包括用嵌入所述驱动控制器的唯一密钥在硬件内加密的装置。

20. 权利要求 19 的系统，其中唯一的密钥被冗余地嵌入所述计算机系统的所述驱动控制器中。

21. 权利要求 17 的系统，还包括让用户能够选择对所述数据进行加密的装置。

22. 权利要求 21 的系统，还包括在存入所述存储媒介的每一个文件中做标记，说明所述数据文件是否需要所述计算机系统进行解密

的装置。

23. 权利要求 16 的系统，其中的加密的装置对于在所述计算机系统上运行的用户应用程序来说是透明的，所述用户应用程序提供所述数据从计算机系统存入存储装置。

24. 权利要求 16 的系统，其中的构造装置包括在软件中为所述计算机系统产生所述唯一密钥，所述产生装置包括确定所述计算机系统至少一个硬件部件的至少一个标识号，并利用这至少一个标识号为所述计算机系统产生所述唯一的密钥。

25. 权利要求 24 的系统，其中的产生装置包括在所述计算机系统一个设备驱动器初始化的时候产生所述唯一密钥，并将所述唯一密钥储存在所述计算机系统中的易失性存储器里的装置。

26. 权利要求 16 的系统，其中的计算机系统和存储媒介都包括计算机的一部分，其中的存储媒介包括不可拆卸计算机存储媒介或者可拆卸计算机存储媒介中的一样。

27. 权利要求 26 的系统，其中的计算机包括膝上型计算机，所述存储媒介包括所述膝上型计算机的计算机硬盘。

28. 权利要求 16 的系统，还包括从所述存储媒介取出所述加密数据，并用所述唯一密钥对加密数据解密的装置，对在所述计算机系统上运行的用户应用程序来说所述解密是透明的。

29. 权利要求 28 的系统，其中的加密装置包括在硬件内用所述唯一密钥进行加密的装置，所述硬件驻留在所述计算机系统的驱动控制器内，其中的解密装置包括在驻留在计算机系统的驱动控制器内的硬件内进行解密的装置。

30. 权利要求 28 的系统，其中的加密装置包括在软件内用所述唯一密钥加密所述数据的装置，这一加密是在该计算机系统一个设备驱动器中的软件内完成的，其中的解密装置包括在软件中用所述唯一密钥解密加密数据的装置，这一解密装置还在所述设备驱动器中的软件内实现，其中的加密和解密对于所述计算机系统上运行的用户应用程序而言是透明的。

31. 一种处理系统，包括：

用于储存数据的一种存储媒介；和

一种计算机系统，用于构造一个唯一密钥，用这个唯一密钥加密

数据产生加密数据，该计算机系统还包括一个设备驱动器和驱动控制器，用于将加密数据存入所述存储媒介.

32. 权利要求 31 的处理系统，其中的计算机系统包括在所述设备控制器中的硬件中实现的一个加密单元和一个解密单元，从而使对要存入所述存储媒介的数据进行加密和对从所述存储媒介取出来的数据进行解密对所述处理系统上运行的应用程序来说是透明的，其中的唯一密钥嵌入在驱动控制器中，供所述加密单元和解密单元使用.

33. 权利要求 31 的处理系统，其中的计算机系统包括一个加密单元和一个解密单元，在所述设备驱动器中用软件实现，从而使对要存入所述存储媒介的数据进行加密和对从所述存储媒介取出来的数据进行解密对所述处理系统上运行的应用程序来说是透明的，其中的唯一密钥是在设备驱动器初始化过程中产生的，储存在易失性存储器里.

34. 至少一个程序存储装置，可以被机器读出来，包括至少一个程序，该程序可以被机器执行，以实现一种方法，用于保护从计算机系统存入存储媒介的数据，包括:

在所述计算机系统内构造一个唯一的密钥;

用这个唯一的密钥加密数据，产生加密数据; 和

将这些加密数据存入所述存储媒介，不将唯一的密钥存入所述存储媒介.

35. 权利要求 34 的至少一个程序存储装置，其中的构造步骤包括在所述计算机系统的硬件内嵌入所述唯一密钥.

36. 权利要求 35 的至少一个程序存储装置，其中的嵌入步骤包括将所述唯一的密钥嵌入所述计算机系统的驱动控制器中.

37. 权利要求 36 的至少一个程序存储装置，其中的加密步骤包括用嵌入所述驱动控制器的唯一密钥在硬件内加密.

38. 权利要求 34 的至少一个程序存储装置，其中的加密对于在所述计算机系统上运行的用户应用程序来说是透明的，所述用户应用程序提供所述数据从计算机系统存入存储装置.

39. 权利要求 34 的至少一个程序存储装置，其中的构造步骤包括在软件中为所述计算机系统产生所述唯一密钥，所述产生步骤包括确定所述计算机系统至少一个硬件部件的至少一个标识号，并利用这

至少一个标识号为所述计算机系统产生所述唯一的密钥。

40. 权利要求 39 的至少一个程序存储装置，其中的产生步骤包括在所述计算机系统一个设备驱动器初始化的时候产生所述唯一的密钥，并将所述唯一密钥储存在所述计算机系统中的易失性存储器里。

41. 权利要求 34 的至少一个程序存储装置，还包括从所述存储媒介取出所述加密数据，并用所述唯一密钥对加密数据解密，对在所述计算机系统上运行的用户应用程序来说所述解密是透明的。

42. 权利要求 41 的至少一个程序存储装置，其中的加密包括在硬件内用所述唯一密钥进行加密，所述硬件驻留在所述计算机系统的驱动控制器内，其中的解密包括在驻留在计算机系统的驱动控制器内的硬件内进行解密。

43. 权利要求 41 的至少一个程序存储装置，其中的加密包括在软件内用所述唯一密钥加密所述数据，这一加密是在该计算机系统一个设备驱动器中的软件内完成的，其中的解密包括在软件中用所述唯一密钥解密加密数据，这一解密还在所述设备驱动器中的软件内进行，其中的加密和解密对于所述计算机系统上运行的用户应用程序而言是透明的。

说　　明　　书

用不可访问的唯一密钥对储存的数据进行加密/解密

总的来说，本发明涉及数据的加密和解密方法，更具体地说，涉及一种技术，它采用专用于计算机系统的不可访问的唯一密钥，对计算机系统储存在这一存储媒介里的数据进行加密和解密，其中的加密和解密采用了专用于这一计算机系统的不可访问的唯一密钥。

对临时或者永久储存的数据，或者通过不安全链路传输的数据，进行加密和解密的程序在本领域里大家都了解一些。多数加密算法采用一个密钥来加密数据。于是，加密算法的成功使用通常都要求接收加密传输的数据或者从存储器读取加密数据的台拥有跟加密数据所用密钥相同的密钥，这样才能解密。因此，任何未经授权的一方都不应当知道也不应当能够获得所用密钥。

加密技术很多，可以用于计算机和计算机数据。但进一步的改进非常必要，特别是在防止未经授权的一方获得密钥的技术方面。

具体而言，对于本发明，计算机数据常常是储存在硬盘上的。如果用硬盘来储存敏感数据，它的丢失或者被盗就会带来危险。尤其是便携式（也就是膝上型）计算机系统，它们常常能够很容易地打开，硬盘的被盗会构成威胁。

因此，在这一领域需要一种加密/解密方法，它对于用户应用程序而言是透明的，构造密钥的基础是主机的唯一属性，这样，不访问这一台计算机就无法对这一台机器中的加密数据解密。

于是，简单地概括起来，一方面本发明包括一种方法，用于保护从计算机存入存储媒介的数据。该方法包括为这一计算机系统构造一个唯一的密钥；用这个唯一的密钥加密数据，以产生加密数据；将加密数据储存在存储媒介上，而不将唯一的密钥储存在存储媒介上。

另一方面，提供了一种方法，用于保护计算机系统储存在存储媒介上的数据。该系统包括在这个计算机系统内确定一个唯一密钥的装置，以及用这个唯一密钥加密数据产生加密数据的装置。还提供了将加密数据储存在存储媒介上的装置，其中储存加密数据的时候不将唯一密钥储存在存储媒介中。

再一方面，提供了一种处理系统，它包括用于储存数据的一种存储媒介和一种计算机系统。该计算机系统用于构造唯一的密钥，并用这个唯一的密钥加密数据来产生加密数据。该计算机系统还包括一个设备驱动器和一个驱动控制器，用于将加密数据储存在存储媒介里。

另一方面，提供了可以被机器读出的至少一个程序存储装置，用于储存至少一个程序，该程序可以被机器执行，以实现保护计算机系统存入存储媒介的数据的方法，该方法包括：在计算机系统内构造唯一的密钥；用这个唯一的密钥加密数据以产生加密数据；将这些加密数据存入存储媒介，而不将这个唯一的密钥存入存储媒介。

换句话说，在所有的实施方案中，提供了一种透明的技术，用于加密和解密计算机系统储存在一种可拆卸或者不可拆卸存储媒介上的数据，比方说储存在硬盘、软盘或者光盘上的数据。这一加密/解密技术采用专用于这一计算机系统的一个唯一、不可获得的密钥。这个密钥，以及加密逻辑和解密逻辑，可以嵌入硬件，例如，计算机系统的驱动控制器中。或者，这一密钥以及加密逻辑和解密逻辑，可以驻留在这一计算机系统的软件中。

如果用软件来实现，这个唯一密钥就可以被例如计算机系统的设备驱动器获得。具体地说，可以对这一设备驱动器编程，使它在启动的时候从计算机系统的不可拆卸硬件部件读取一个或者多个序列号（或者象 PCI 配置信息、芯片识别号等等这样的其它静态信息）。然后可以将这些序列号组合（例如混编）成唯一密钥，从而保证这一计算系统加密的数据只能由该计算机系统解密。

这里提供的透明加密/解密方法能够保证例如硬盘、软盘或者光盘上的数据只能在储存这些数据的特定的机器里使用。如果这一储存媒介重新装入另一台机器，这一媒介就无法使用。显然这对于便携式计算机用户、军方用户或者有敏感数据要保护的用户来说特别有意义。这一加密和解密方法最好采用基于主机属性的密钥，因此，不用这一台主机解密就无法使用。此外，根据本发明，构造这个唯一的密钥时，不需要从计算机外部提供任何种子数。

通过下面对本发明特定优选实施方案的详细介绍，同时参考以下附图，前面介绍的本发明的目的、优点和特征，以及其它目的、优点和特征，将更加容易理解。在这些附图中：

图 1 描述了实现本发明的原理中加密/解密能力的一个计算机系统的实施方案，其中的加密/解密能力是用一个嵌入的密钥在硬件里实现的。

图 2 介绍了实现按照本发明的原理的加密/解密能力的一个计算机系统的另一个实施方案，其中的密钥是在主机系统唯一属性的基础之上产生的，加密/解密能力是在软件里实现的。

图 3 是按照本发明的原理在软件中产生密钥的一个实施方案的流程图；

图 4 是储存按照本发明的能力加密的数据的一个实施方案的流程图；和

图 5 是取出按照本发明的能力加密的数据的一个实施方案的流程图。

一般而言，这里提出的是将数据加密，储存在可拆卸或者不可拆卸媒介上的一种更加安全的方法。数据保护是这样来实现的：获得一个唯一的号码，嵌入计算机内，写入（或者拥有）数据存储媒介，这个号码是嵌入存储媒介中而不是在存储媒介中的；用这个唯一的号码作为加密基础，对数据加密；加密以后，将加密数据储存在数据存储媒介里，而不将这个唯一的号码存储在数据存储媒介里。不可拆卸的存储媒介可以包括计算机的硬盘，而可拆卸的媒介可以包括软盘、可写光盘等等。通过用对储存这些数据的这一特定计算机来说是唯一的密钥加密数据，这些加密数据只能由同一台计算机解密。

这个唯一的密钥可以包括储存在计算机一个不可拆卸部件里的一个号码，或者这个密钥可以通过混编（或者用其它的数学组合方法）不可拆卸部件中的一个或者多个号码。例如，这个唯一的号码可以使嵌入计算机处理器，或者集成在主板上其它部件的一个序列号。但是有一个要求，用作密钥基础的这个号码不能跟加密数据储存在同样的媒介上。

存储以前对数据进行加密，以及从存储器中取出数据以后对数据进行解密，这些事情可以在硬件里也可以在软件里完成。图 1 描述了一个计算机系统的一个实施方案，该计算机系统笼统地用 10 来标识，其中的密钥以及加密和解密单元都是嵌入计算机中每一个驱动控制器 20 里的硬件。利用储存在驱动控制器 20 中的唯一密钥 30，硬件加

密和解密既可以在驱动控制器 20 里进行（如图所示），又可以在驱动器自己内部进行。

如图 1 所示，计算机系统 10 还包括一个处理器 12，它运行一个用户应用程序 14，执行一个文件系统 16，并运行一个设备驱动器 18。众所周知，存储系统依赖于软件，其中每一个驱动器都有一个有关的“文件系统”16，它包括，叫做“设备驱动器”18 的软件等等．设备驱动器是低级可执行模块，能够访问（例如读和写）计算机的硬件部件。

在图 1 所示的实施方案里，假设密钥 30、加密单元 32 和解密单元 34 都是用驱动控制器 20 里的硬件来实现的．许多个人计算机都有“驱动控制器”，它控制着数据流向和来自磁盘驱动器、软盘驱动器等等．驱动控制器的常用类型包括 IDE（集成驱动电子）、SCSI（小型计算机系统接口）和软盘驱动控制器．

密钥可以嵌入驱动器或者驱动控制器的逻辑中．流行的驱动控制器常常都是集成在具有多种功能的一个芯片中．例如，一块芯片可以用作一个 PCI 到 ISA 的总线桥，包括一个或者多个 IDE 驱动控制器，和一个中断控制器，直接存储器存取（DMA），一个或者多个通用串行总线（USB），电源管理，和其它功能．这种芯片的一个实例是英特尔的 82371AB PCI 到 ISA/IDE 的 Xcelerator（PIIX4）多功能芯片．密钥可以储存在一个只读存储器里（或者几个寄存器里，为了冗余的目的），从外部无法访问它——也就是说，外部世界无法知道它的内容．密钥将在内部访问，并用于多路复用数据以便传输的时候控制数据，例如，通过一条外部总线发往可记录 CD-ROM、软盘等等这样的存储媒介．密钥可以通过一个线性反馈移位寄存器（LFSR）用一个时钟信号周期性地激励它而不断变化．准备数据在一个外部总线上传输，传递给系统的主存储器（DRAM）或者另一个存储媒介，在那里它将作为普通未加密数据的时候，解密单元会访问同一个密钥并用它反过来重复加密过程。

根据本发明的一个实施方案，当数据存入存储装置 22 的时候，硬件 32 用唯一的密钥自动地加密数据，而从存储装置 22 中取出数据的时候，解密单元 34 用密钥 30 自动地对加密数据解密．任意的传统加密/解密技术都可以用于加密单元 32 和解密单元 34，只要这种技术

采用加密/解密密钥。作为一种加强，系统可以提供一个用户选择输入 35，有选择地控制加密单元 32 对储存在存储装置 22 上的数据加密还是不加密。这一可选用户输入可以由本领域里的技术人员根据计算机系统 10 的具体情况用硬件或者软件来实现。

实现本发明的概念的另一种方法是在高于硬件的级别上加密和解密数据，也就是高于驱动控制器 20 的级别上。例如，可以在访问驱动器的设备驱动器中用软件实现加密和解密以及密钥的产生。这种方法，这里叫做软件方法，在图 2 里描述。

在图 2 所示的实施方案中，计算机系统 100 包括一个处理器 112，它运行这一个用户应用程序 114、文件系统程序 116 和至少一个设备驱动器模块 118。设备驱动器模块 118 包括一个密钥生成例程 130，以及加密 132 和解密 134 软件。对于硬件方案，本领域里的技术人员可以为用户提供是否对所选数据 135 进行加密的选择。这样，根据用户是否选择加密，图中的数据通过加密单元 132 进入驱动控制器 120 或者在加密单元外面通过。此外，本领域里大家都知道的加密/解密算法可以由本领域里的技术人员跟本发明一起使用，只要这一加密/解密算法采用了加密/解密密钥。加密数据由驱动控制器 120 转发给存储装置 122。

在软件方法中，密钥可以在计算机启动的时候获得（下面进一步介绍）。例如，在一种实施方案中，密钥可以储存在易失性（也就是临时）存储器中，关闭计算机电源的时候会丢失。

通过让用户能够选择是否对特定的数据进行加密，可以让用户决定这些数据可以在其它计算机系统上读出来，还是只能在写入存储媒介的计算机系统上读出来。此外，配备了这种加密/解密能力选择的驱动器（或者驱动控制器或者设备驱动器），可以给每一个文件做上标记，从而在从存储媒介读取文件的时候，这个文件是否需要解密是十分清楚的。

图 3～5 综述了本发明加密/解密能力软件实施中采用的过程。在图 3 里，产生一个唯一的密钥，例如，在设备驱动器初始化的时候，通过访问计算机系统 300 的不可拆卸装置/部件的机器专用信息来产生。利用这些信息，通过例如混编这些信息 310 来产生密钥，在这以后，密钥储存在设备驱动器的易失性存储器 320 中。

典型计算机上有许多芯片都是以一种不可拆卸的方式安装在主电路板，或者母板上。这种芯片可以包括主处理器（奔腾处理器之类），一个视频芯片（或者显示适配器），一个音频芯片，连接处理器主总线的一个或者多个适配器，一个外围部件互连（PCI）总线，主存储器（DRAM），加速图形端口（AGP），驱动控制器，总线桥等等。这些芯片可以包括不变的可读信息，比方说芯片 ID 或者序列号。此外，许多芯片都是 PCI 设备——也就是说，它们是用 PCI 总线连接起来的。PCI 本地总线规范规定了一个强制性的配置空间，由跟这一总线连接的所有设备实现。这一配置空间有一个 16 字节的预定义报头区域，后面是两种辅助空间中的一种。该报头区域包括几个常数字段，它们可以被低级代码（比方说设备驱动器）访问。在这些字段中有设备 ID，销售商 ID，版本 ID，分类码和报头类型。这些或者其它可以被一贯地访问的不可拆卸部件的静态记录，可以被读出，它们的内容可以组合起来构成一个“指纹”，这个号码可以用作密钥。

一旦建立好密钥，就可以选择将数据加密储存。如图 4 所示，设备驱动器最初接受一个储存数据的请求 400，然后查询是否选择了加密 410。如果是这样，就用例如在设备驱动器初始化的过程 420 中产生的密钥加密数据。然后将加密数据发送给存储装置 430。如果用户没有选择加密，就将数据直接发送给存储装置。

图 5 描述了取数操作的一个实施方案，它开始于设备驱动器收到一个数据请求 500。数据是从存储装置中取出来的 510，处理过程判断出这些数据是不是加密数据 520。如果是这样，就用设备驱动器初始化的过程中产生的唯一密钥对这些数据进行解密。解密以后，或者如果数据没有加密，将数据发送给请求发出方 540。

概括起来，这里提供的是一种技术，其中嵌入的或者获得的一个号码对于这一计算机系统来说是唯一的。通过实例说明，这个号码可以包括这一计算机系统中特定不可拆卸部件的序列号或者其它识别号。或者，制造计算机的时候可以有一个“一次写入”区域，可以由用户或者在制造的时候写入一个唯一的值。然后，当用户储存数据时访问这个唯一的密钥，将它用于加密数据或者解密加过密的数据。加密和解密最好在计算机系统的较低级别进行，也许由输入/输出（I/O）子系统，按照类似于数据压缩方式的方式进行。此外，可以

让用户选择禁止加密.

密钥和加密、解密单元可以用硬件实现，也可以用软件实现，就象前面讨论过的一样．在这两种方式中，构成加密和解密基础的唯一密钥并不储存在存储装置里．这里提供的是一种加密/解密技术，这种技术是基于主机属性的，也就是说，用来加密/解密数据的密钥对于嵌入机器的一个号码或者从机器不可拆卸部件中获得的一个号码而言，是唯一的．这样，这一加密/解密对于用户来说可以是透明的，用户不必卷入到加密/解密过程中去．此外，不需要从外界提供任何种子数字给计算机.

在加密之前，这个唯一的密钥可以提供给远处的系统制造商或者由他们取过去，记录下来．这样，如果发生灾难性的故障，比方说主板故障（例如），利用记录下来的唯一号码，硬驱动仍然可以在别的地方将数据内容解密出来，尽管唯一地加密了数据的计算机系统发生了故障.

本发明可以包括在例如，产品中（例如一个或者多个计算机程序产品），其中有例如计算机可以使用的媒介．这一媒介中嵌入了例如计算机可以读出来的程序代码装置，用于提供和支持本发明的能力．该产品可以作为计算机系统的一部分，或者单独销售.

另外，至少可以提供一个计算机可以读的程序存储装置，其中嵌入计算机可以执行的至少一个程序，以实现本发明的能力.

提供这里描述的流程图的目的只是为了进行说明．这些图可以有些变化，或者其中的步骤（或者操作）可以有些变化，而不会偏离本发明的实质．例如，在某些情况下，这些步骤可以以不同的顺序来执行，或者其中的一些步骤可以被删除或修改，或者添加一些步骤．所有这些改变都属于本发明的范围.

尽管按照本发明的特定优选实施方案详细描述了本发明，但是本领域里的技术人员可以对它进行许多的改进和修改．因此，以下权利要求的目的是覆盖所有这种改进和修改，只要它们属于本发明的实质和范围之内.

说 明 书 附 图

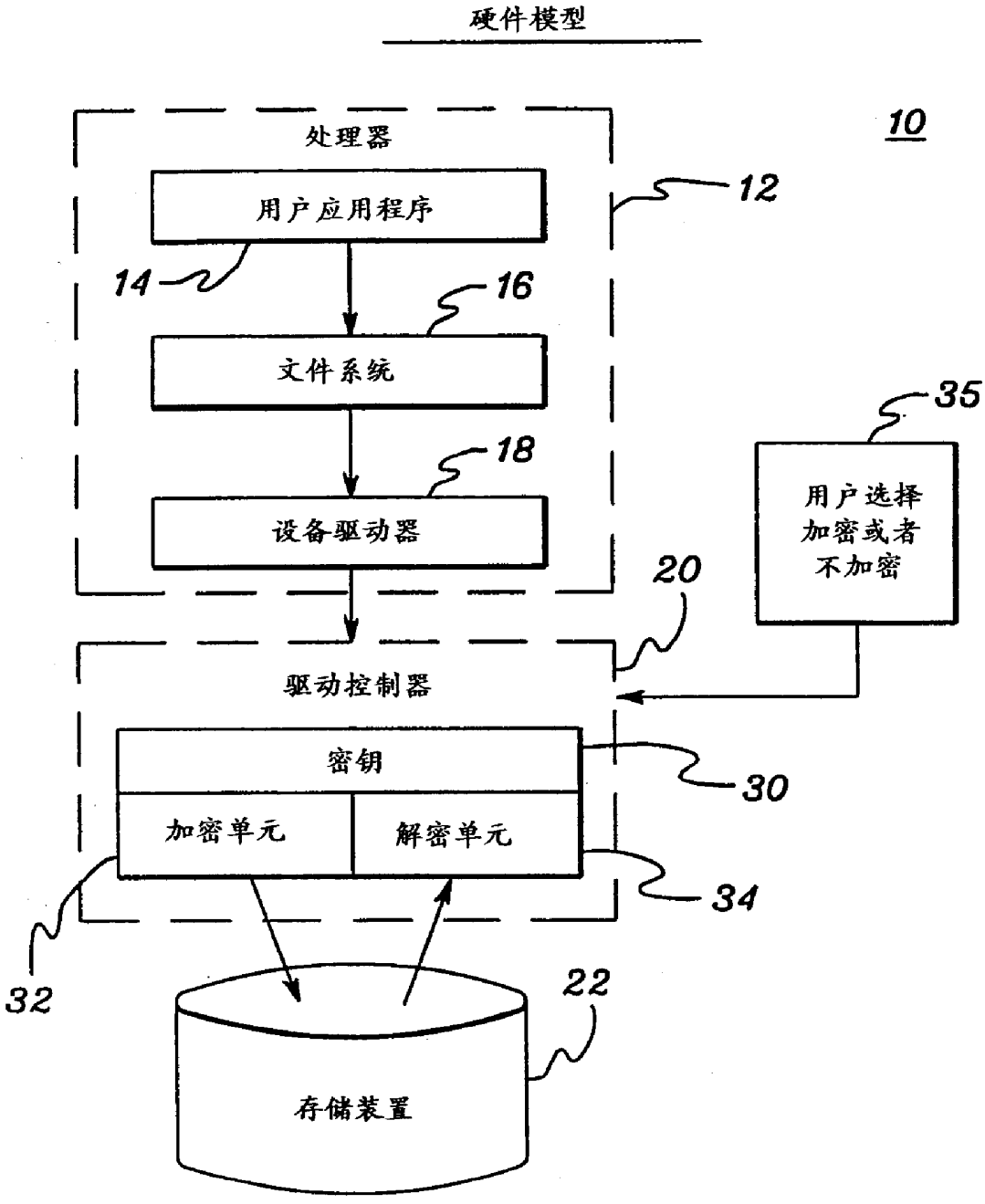

硬件模型
处理器
10
用户应用程序
12
14
16
文件系统
35
18
设备驱动器
用户选择
加密或者
不加密
20
驱动控制器
密钥
30
加密单元
解密单元
34
32
22
存储装置

图 1

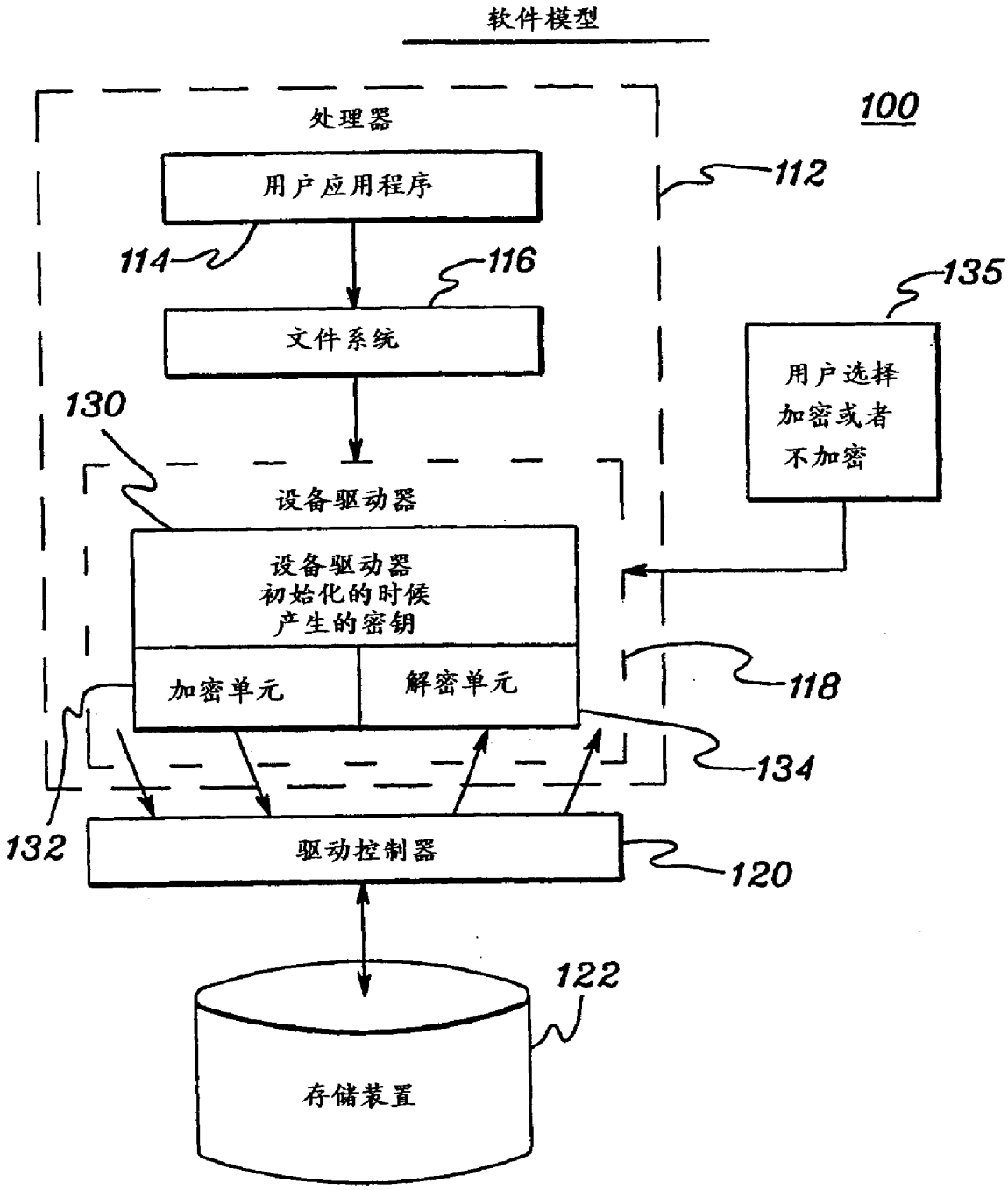

软件模型
处理器
100
用户应用程序
112
114
116
文件系统
135
用户选择
加密或者
不加密
130
设备驱动器
设备驱动器
初始化的时候
产生的密钥
加密单元
解密单元
118
134
132
驱动控制器
120
122
存储装置

图 2

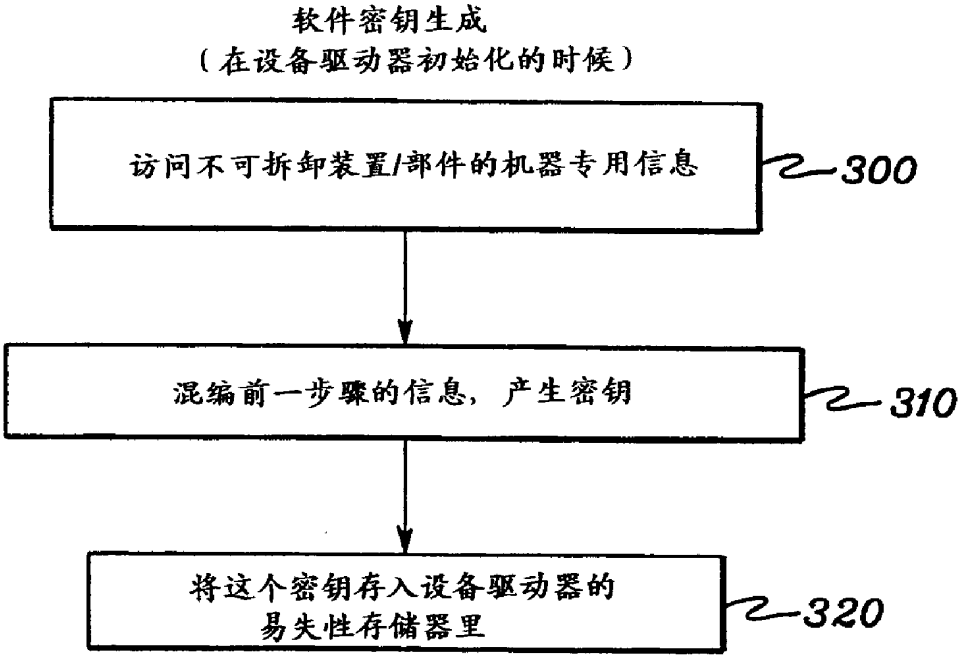

软件密钥生成
（在设备驱动器初始化的时候）
访问不可拆卸装置/部件的机器专用信息
300
混编前一步骤的信息，产生密钥
310
将这个密钥存入设备驱动器的
易失性存储器里
320

图 3

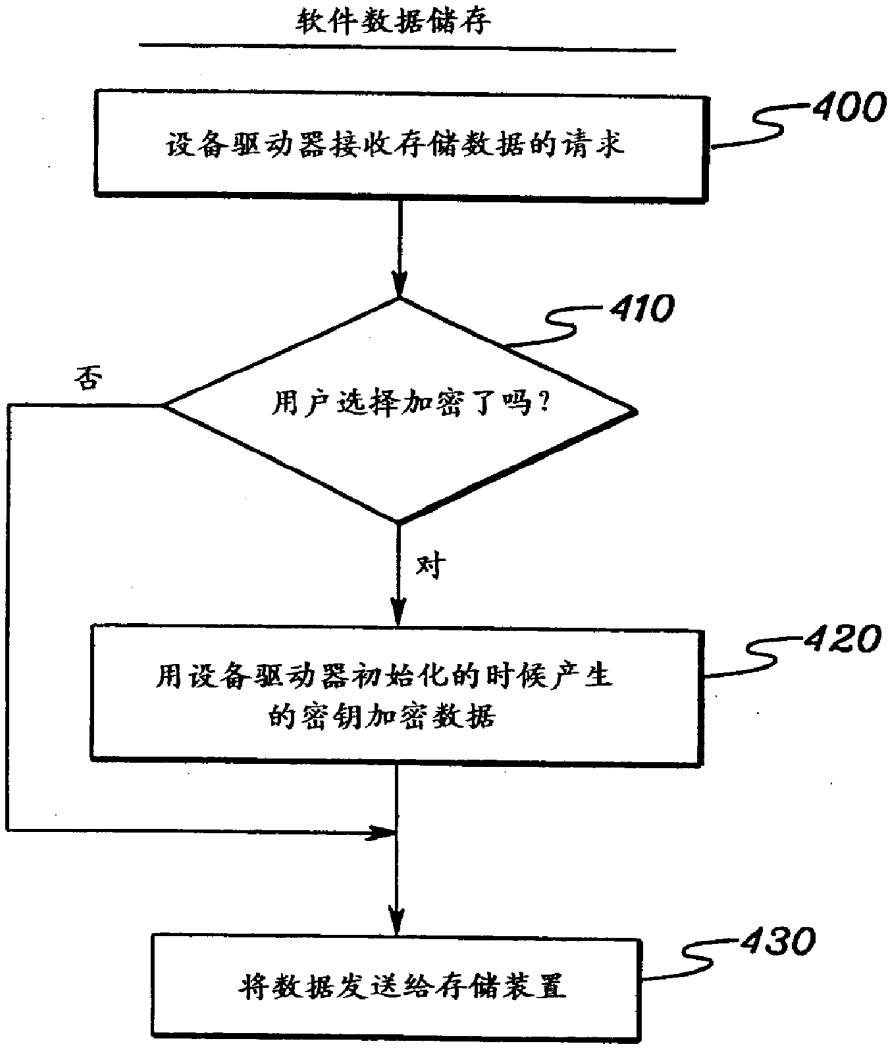

软件数据储存
设备驱动器接收存储数据的请求
400
410
用户选择加密了吗？
否
对
用设备驱动器初始化的时候产生
的密钥加密数据
420
将数据发送给存储装置
430

图 4

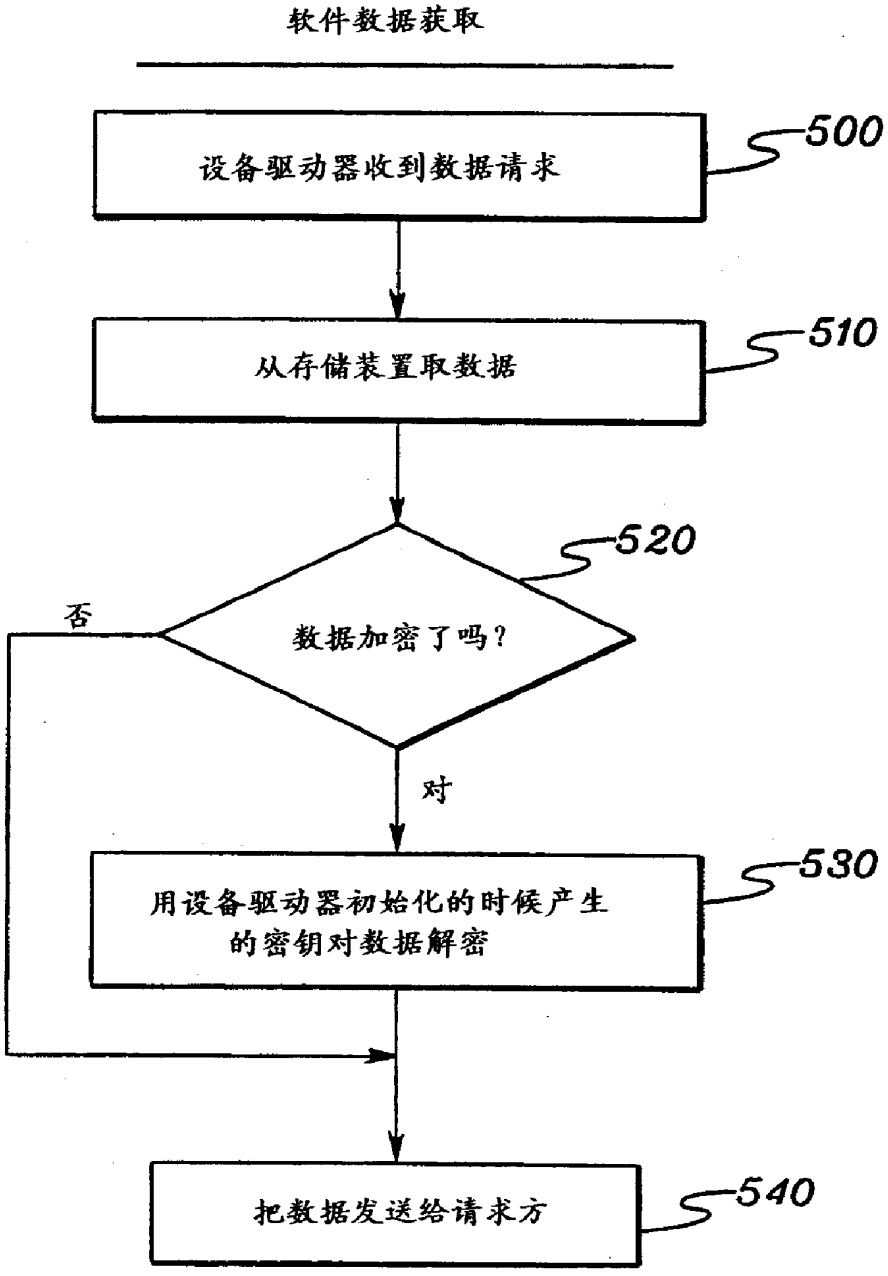

软件数据获取
设备驱动器收到数据请求
500
从存储装置取数据
510
520
数据加密了吗？
否
对
用设备驱动器初始化的时候产生
的密钥对数据解密
530
把数据发送给请求方
540

图 5